



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/048,057	01/25/2002	Michel Habert	T2147-907642	8724

181 7590 12/15/2006

MILES & STOCKBRIDGE PC  
1751 PINNACLE DRIVE  
SUITE 500  
MCLEAN, VA 22102-3833

EXAMINER
----------

SHIFERAW, ELEN I A

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 12/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

10/048,057

Applicant(s)

HABERT, MICHEL

Examiner

Eleni A. Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE \_\_\_\_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 26 September 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_.

## DETAILED ACTION

### *Response to Amendment and Argument*

1. Applicant's amendments and arguments filed 09/26/2006 have been fully and moot in view of new grounds of rejections.

### *Claim Rejections - 35 USC § 103*

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 4-9, 11, and 14-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brody et al. 6,278,697 B1 in view of Kailamaki et al. Pub. No.: US 2002/0146018 A1.

Regarding claim 1, Brody et al. discloses a method for secure communication between first and second entities interconnected via an internet network, said entities being associated with respective first and second processing systems connected to said internet network, said first system operating in client mode and said second system operating in server mode (fig. 9), said method comprising:

assigning respective permanent internet addresses to said first and second entities (col. 3 lines 26-29; *first and second communication identity*),

making at least one application, located in a server of said second system, accessible to said first entity (fig. 9 elements 369 and 368; *first and second communication protocol server*),

receiving an application request at the second system (col. 4 lines 66-col. 5 lines 9),

selectively recognizing said application request as belonging to one of a first and a second communication protocol, said first communication protocol associated with a first server of the second system and said second communication protocol associated with a second server of the second system (fig. 9 and col. 9 lines 60-col. 10 lines 34; *first communication protocol server, second communication protocol server and communication switch in a single server*),

providing said application request recognized as belonging to the first communication protocol to the first server of the second system (col. 10 lines 3-33 and col. 3 lines 21-56),

providing said application request recognized as belonging to the second communication protocol to the second server of the second system (col. 10 lines 3-33 and col. 3 lines 21-56),

converting, using a web server application interface portion of the second server, said application request recognized as belonging to the second communication protocol to first communicate protocol (abstract, fig. 16 element 436, and claim 1), and

said second entity hosting a WAP gateway utilizing the web server application interface and said second system is configured to communicate, via the web server application interface adapter, directly with a first type of WAP application and via a web container and at least one specific application program interface with a servlet WAP application (col. 3 lines 20-34, fig. 9 and fig. 2; *converting/interfaces multiple plurality of protocols i.e. CDMA, TDMA, and GSM in a single server*).

Brody et al. fails to disclose encrypting data exchanged between said first and second entities in conformity with a desired security protocol, wherein said first and second systems include a communication protocol stack having at least one layer which allows for said encrypting step to be performed, and

the protocols being a WAP protocol and WEB protocol.

However, Kailamaki et al. discloses encrypting data exchanged between said first and second entities in conformity with a desired security protocol, wherein said first and second systems include a communication protocol stack having at least one layer which allows for said encrypting step to be performed (0002, 0023, 0038, and 0315), and

the protocols being a WAP protocol and WEB protocol (0012-0027, 0281-0286, 0315, and 0036-0037; *a WAP gateway **SERVER** converting/interfaces WAP protocol and WEB protocol*).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Kailamaki et al. within the system of Brody et al. because they are analogous in wireless communication. One would have been motivated to incorporate the teachings of Kailamaki et al. because it would interface the specific protocol WAP(WTLS) with WEB(WML) or vice versa in a single server to securely provide documents to requesters.

Regarding claim 11, Brody et al. discloses a system architecture for secure communication between first and second entities interconnected via an internet network, said entities respectively being associated with first and second data processing systems within a set of distributed systems connected to said internet network, said first system operating in client mode and said second system operating in server mode, said first and second entities being associated with permanent internet addresses, comprising:

at least one application included in said second system, said at least one application being accessible to said first entity (col. 3 lines 26-29; *first and second communication identity*);

first and second communication protocol stacks respectively included in said first and second systems (col. 3 lines 21-34 and fig. 9; *GSM protocol stack, CDMA protocol stack, and CDMA protocol stack*)

said first communication protocol associated with a first server of the second system and said second communication protocol associated with a second server of the second system (fig. 2 elements 158, 160, 162, fig. 9 elements 368-369),

said second server comprising a web server application interface portion configured to convert an application request belonging to the second communication protocol to the first communication protocol (abstract, fig. 16 element 436, and claim 1), and

each of said first and second communication protocol stacks comprising at least one address layer using a respective one of said permanent IP addresses (col. 3 lines 26-29; *first and second communication identity*) and said second entity hosting a WAP gateway utilizing the web server application interface adapter and the server included in said second system is configured to communicate, via the web server application interface adapter, directly with a first type of WAP application and via a web container and at least one specific application program interface with a servlet WAP application (col. 3 lines 20-34, fig. 9 and fig. 2; *converting/interfaces multiple plurality of protocols i.e. CDMA, TDMA, and GSM in a single server*).

Brody et al. fails to disclose a logical layer for encrypting, in end-to-end mode in conformity with a given security protocol, data exchanged between said first and second entities and the protocols being a WAP protocol and WEB protocol.

However, Kailamaki et al. discloses a logical layer for encrypting, in end-to-end mode in conformity with a given security protocol, data exchanged between said first and second entities (0002, 0023, 0038, and 0315), and

the protocols being a WAP protocol and WEB protocol (0012-0027, 0281-0286, 0315, and 0036-0037; a WAP gateway **SERVER** converting/interfaces WAP protocol and WEB protocol).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Kailamaki et al. within the system of Brody et al. because they are analogous in wireless communication. One would have been motivated to incorporate the teachings of Kailamaki et al. because it would interface the specific protocol WAP(WTLS) with WEB(WML) or vice versa in a single server to securely provide documents to requesters.

Regarding claim 4 Kailamaki et al. discloses a method wherein said encrypting step is performed in conformity with an IPsec protocol in tunnel mode, in order to obtain secure data exchanges between said first and second entities, and wherein said IPsec protocol is used with an EPS mechanism for authenticating information sources (0002, 0023, 0038, and 0315; *WTLS... SSL*). One ordinary skill in the art would have combined this at the time of the invention because IPsec is a secure encryption protocol to encrypt communication between two entities.

Regarding claim 5 Brody et al. discloses a method, wherein said first entity is a user of said first system, wherein said method further includes a step for authenticating said user, and wherein said permanent IP address assigned to said first entity is used to identify said user (col. 4 lines 66-col. 5 lines 9).

Regarding claim 6 Kailamaki et al. discloses a method wherein the combinations through said network take place in data packet mode, and wherein said permanent IP address identifying said user is present in encrypted form in conformity with said IPsec protocol, in each of said data packets (0002, 0023, 0038, and 0315; *WTLS... SSL*).

Regarding claims 7 and 15, the combination discloses a method wherein said first system is connected to a wireless transmission segment,

wherein communications between said first system and said second system take place in conformity with a WAP protocol (Brody et al. fig. 9 elements 368-369, and Kailamaki et al. 0012-0027, 0281-0286, 0315, and 0036-0037), and

wherein said second system includes a WAP server and a unified interface between said WAP server and at least one application, said at least one application being located in said second system and being accessible by said first entity (Brody et al. fig. 9 elements 368-369, and Kailamaki et al. 0012-0027, 0281-0286, 0315, and 0036-0037), and

wherein the WAP server is integrated into said second system as a web server (Brody et al. fig. 9 elements 368-369, and Kailamaki et al. 0012-0027, 0281-0286, 0315, and 0036-0037). The rationale for combining are the same as claim 1 above.

Regarding claim 8 Brody et al. discloses a method wherein said second system includes an additional module for performing two-way interface adaptation of structures, which makes it possible to support application interfaces used by web servers (col. 9 lines 60-col. 10 lines 33).

Regarding claim 9, Kailamaki et al. discloses a method wherein said first system includes a WAP browser (abstract).

Regarding claim 14, Kailamaki et al. discloses architecture, wherein said logical layer in each of said first and second protocol stacks conforms to an IPSec protocol in tunnel mode, in order to obtain secure data exchanges between said interconnected first and second entities, and wherein



Art Unit: 2136

said IPSec protocol is used with an EPS mechanism for identifying information sources (0002, 0023, 0038, and 0315; *WTLS... SSL*). One ordinary skill in the art would have combined this at the time of the invention because IPSec is a secure encryption protocol to encrypt communication between two entities.

Regarding claim 16, Kailamaki et al. discloses architecture, wherein said second system includes at least one additional module for two-way conversion of packets of structures in conformity with web or WAP protocols (col. 9 lines 60-col. 10 lines 33).

Regarding claim 17, Kailamaki et al. discloses architecture, wherein said first system is a mobile telephone terminal operating in a GSM standard, said mobile telephone terminal including a WAP type browser constituting a client and a display screen for displaying pages in WML-type language (0281).

Regarding claim 18, Kailamaki et al. discloses architecture, wherein said first system is a mobile telephone terminal operating in a GPRS standard, said mobile telephone terminal including internet browser constituting a client and a display screen for displaying pages in WML-type language (0281, fig. 0014, 0023).

3. Claims 2-3, 10, and 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brody et al. 6,278,697 B1 and Kailamaki et al. Pub. No.: US 2002/0146018 A1 and further

Art Unit: 2136

in view of W. Stallings, 1999 (Stallings, "Cryptography and Network Security, Principles And Practice, 2<sup>nd</sup> edition.")

As per claims 2 and 12, Brody et al. and Kailamaki et al. disclose all the subject matter as described above. Brody et al. and Kailamaki et al. fail to disclose a method, wherein said permanent IP addresses assigned to said first and second entities conform to an IPV6 Internet address protocol. However Stallings teaches a method, wherein said permanent IP addresses assigned to said first and second entities conform to an IPV6 Internet address protocol (Stallings page 400 section 13.1 par. 3). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the plurality of protocols in the combination system of Brody et al. and Kailamaki et al. with a different protocol like IPV6 and Ipv4 to use a different security protocol.

As per claim 3, Stallings further teaches a method, wherein communications through said internet network take place in conformity with an IPV4 Internet address protocol, and wherein said method further comprises:

executing, in at least one of said first and second systems, an address conversion step which includes converting said IPV4 internet address protocol to said IPV6 internet address protocol (Stallings page 400 section 13.1 lines 16-19, and page 405 lines 14-16). The rationale for combining are the same as claim 2 above.

As per claim 10, Stallings and WAP forum further teach all the subject matter as described. In

Art Unit: 2136

addition, WAP forum teaches a method, wherein said first system includes a mobile system, wherein said method further includes assigning to said first system a temporary address, and initiating a dialog between said first system and a home agent connected to said internet network to correlate said permanent address assigned to said first entity with said temporary address, in conformity with said IPV6 protocol (WAP forum pages 23-24 section 705, and fig. 6). The rationale for combining are the same as claim 2 above.

As per claim 13, Stallings and WAP forum teach all the subject matter as described above. In addition Stallings teaches an architecture, wherein said internet network conveys data packets in conformity with an IPV4 protocol,

wherein each of said first and second protocol stacks includes a first address layer in the IPV6 protocol and a second address layer in the IPV4 protocol from which PV6-compatible addresses are derived, in order to obtain exchanges in tunnel mode (Stallings page 400 section 13.1 lines 16-19, and page 405 lines 14-16), and

wherein said logical layer in each of said first and second protocol stacks encrypts data packets exchanged between said first and second entities (Stallings section 13.1-13.2). The rationale for combining are the same as claim 2 above.

### *Conclusion*

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

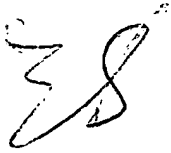
5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


Application/Control Number: 10/048,057  
Art Unit: 2136

Page 12

A handwritten signature, possibly reading 'ES', in dark ink.

December 8, 2006

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

A handwritten signature in dark ink, appearing to be 'Nasser Moazzami'.  
12,8,06